

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Jeffrey Carter, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant to obtain the recordings of virtual meetings conducted on the BlueJeans by Verizon platform associated with the BlueJeans IDs 169152207, 2336004334, 2483755327, or 9164987431 (jointly referred to hereinafter as Target Accounts), stored at premises owned, maintained, controlled, or operated by Verizon Communications (Verizon), an electronic communications service and/or remote computing service provider headquartered at 180 Washington Valley Road, Bedminster, NJ 07921, which meet the following limiting criteria:

- a. The virtual meetings from the Target Accounts which occurred between August 1, 2018, and November 30, 2018, and which included both Jonathan Link and Marcel Mascarenhas as participants;
- b. The virtual meeting(s) associated with the BlueJeans ID 2483755327, which occurred on March 15, 2019, at or around 4:05 pm Eastern Daylight Time; and
- c. any subscriber information associated with the Target Accounts as related to the recordings referenced in paragraphs 1(a) and (b).

The recordings of the virtual meetings described in 1(a) and (b) above are jointly referred to hereinafter as **Target Recordings**.

2. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Verizon to disclose to the government copies of the information (including the content of communications) further

described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. I am a Special Agent with the United States Department of Labor, Office of Inspector General (DOL-OIG) and have been so since August 2001. I am currently assigned to the Roanoke Field Office. I am a graduate of the Criminal Investigator Training Program at the Federal Law Enforcement Training Center. I have a Bachelor of Science in Criminal Justice. I have more than 20 years' experience conducting criminal investigations involving matters of fraud, theft, conspiracy and false statements. I am a law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses. While assigned to the Roanoke Field Office, I have conducted criminal investigations of individuals, organizations and businesses.

4. I am a co-case agent on the investigation described herein. My co-case agent is Jim Powers, an Investigator with the West Virginia Commission on Special Investigations (hereinafter CSI). The facts in this affidavit come from my personal observations, my training and experience, information obtained from CSI Investigator Powers, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that David Gerald Minkkinen (Minkkinen) and Sivaraman Sambasivam (Sambasivam) conspired to commit trade secret theft in violation of 18 U.S.C.

§ 1832(a)(5) and wire fraud in violation of 18 U.S.C. § 1349 (18 U.S.C. § 1343); and made false statements to a federal agent in violation of 18 U.S.C. § 1001(a)(2). Additionally, on May 31, 2023, a federal grand jury found probable cause to return a superseding indictment charging defendants Minkkinen and Sambasivam with the above identified offenses in case no.

2:22-cr-00163.<sup>1</sup> Based on the facts set out herein, there is probable cause to search the Target Accounts for the **Target Recordings** and related subscriber information as further described in Attachment A, for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

### **JURISDICTION**

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **PROBABLE CAUSE**

#### **Relevant Entities, Executives, and Products**

7. Deloitte is an international company that provides various financial and advisory services, including unemployment claims management services. Deloitte uses a proprietary web-based software platform named Unemployment Framework for Automated Claim & Tax Services (uFACTS) to process unemployment insurance (UI) claims for state agencies. Deloitte

---

<sup>1</sup> On June 26, 2023, the district court dismissed ten counts of the superseding indictment based upon a finding of pre-indictment delay. The order dismissed all charges against defendant Sambasivam, and left four counts charging defendant Minkkinen with violations of 18 U.S.C. § 1001(a)(2). The government timely filed a notice of interlocutory appeal, and on October 10, 2023, filed its brief with the Fourth Circuit Court of Appeals.

considered the uFACTS source code, database, use cases, software designs, schema, logic, artifacts, and architecture to be trade secrets and its proprietary information.<sup>2</sup>

8. Sagitec Solutions (Sagitec) is a global “technology solutions” company headquartered in Saint Paul, Minnesota. Founded in 2004, Sagitec provides a variety of IT products to private and public institutions.

9. The states of Massachusetts and New Mexico were UI clients of Deloitte’s, but not of Sagitec Solutions.

10. Between June 2013 and December 2015, approximately eleven Deloitte employees left Deloitte to work for Sagitec, or worked at Deloitte prior to being employed at Sagitec. Defendant David Gerald Minkkinen (Minkkinen) transitioned in July 2013, followed by defendant Sivaraman Sambasivam (Sambasivam) in September 2013. Immediately after Minkkinen’s arrival in 2013, Sagitec launched its UI practice.

11. Before joining Sagitec, Minkkinen was the UI Practice Leader at Deloitte from May 2009 to June 2013, and Sambasivam served as the lead system architect for the uFACTS Solution Framework at Deloitte from April 2009 until September 2013. Pursuant to their employment agreements with Deloitte, Minkkinen and Sambasivam, and other prior Deloitte employee-co-conspirators, promised to not disclose any Deloitte trade secrets or any other confidential information, and they agreed to return any such information to Deloitte when they separated from the company.

---

<sup>2</sup> CSI Investigator Powers advised Affiant that Deloitte advised him (CSI Investigator Powers) that it took reasonable steps to maintain the secrecy of its trade secrets, along with other associated confidential and proprietary information. In addition, Deloitte’s trade secrets and confidential and proprietary information derive independent economic value from not being generally known to, and not being readily ascertainable through proper means by, the public.

12. When separating from Deloitte, Minkkinen received by email a Deloitte Partner/Principal resignation checklist, which contained sections entitled “Your Obligation to Return Computer and Software Equipment” and “Your Obligation to Return Client Work Papers Belonging to the Deloitte U.S. Firms and Their Clients.” The checklist stated that “[y]ou should not copy client or Deloitte information off your equipment.” The checklist also directed that the partner/principal must “[r]eturn all records checked out in your name in the Deloitte Records Management System (DRMS) to Central Files,” and that “[a]ll work in progress files (not checked out to you in DRMS) should be returned to Deloitte in accordance with directions you receive from your leadership.”

13. During his separation from Deloitte, from July 16 - 19, 2013, Minkkinen and Deloitte employees exchanged emails wherein Minkkinen requested files from his Deloitte computer, to include “Outlook PST files, Outlook contacts, Outlook notes, and Outlook calendar.” In these email communications, Minkkinen stated that he understood the admonishment that the files “should only be personal information” and asserted that he “did not request any proprietary information.” The government obtained a copy of the Outlook PST files dating back to 1999 that Minkkinen took from his Deloitte computer. Minkkinen’s Outlook PST files contained hundreds of emails containing and discussing Deloitte documents, a large percentage of which constituted Deloitte proprietary data.<sup>3</sup>

14. Both before and after their departures from Deloitte, Minkkinen and Sambasivam, and other co-conspirators copied, downloaded, obtained, and transmitted numerous Deloitte files,

---

<sup>3</sup> Per LinkedIn.com, Minkkinen was a partner with KPMG from 1994 to 2000, a Managing Director with BearingPoint from 2000 to 2008, and a principal with Deloitte from 2009 to June/July 2013. (<https://www.linkedin.com/in/david-minkkinen-9a593116/>). In 2002, KPMG changed its name to BearingPoint. (<https://www.bizjournals.com/dallas/stories/2002/09/30/daily30.html>). In 2009, Deloitte purchased BearingPoint’s North American public service unit. (<https://www.bizjournals.com/washington/stories/2009/09/07/story8.html>).

including trade secret information such as uFACTS source code, data, and use cases, without authorization and in violation of their Deloitte employment contracts. These files were subsequently used by numerous Sagitec employees to design, develop, and market Sagitec's UI software, known as "Neosurance."

### **Theft of Trade Secrets and Intellectual Property**

15. The following examples are a sample of the communications between Minkkinen, Sambasivam, and other Sagitec employees regarding their possession and use of Deloitte data.

- a. On or about July 18, 2013, Minkkinen sent an email to a Sagitec employee, attaching a 37-page executive summary from a Deloitte response to a UI request for proposal ("RFP").
- b. On or about July 29, 2013, Minkkinen emailed a Deloitte marketing brochure to Sagitec employees, stating that "I took one of our existing collateral pieces and customized."
- c. On or about August 16, 2013, Minkkinen sent emails to Sambasivam, who was still employed by Deloitte, and a Sagitec employee, attaching Deloitte PowerPoint presentations with the file names "WI UI Fraud Analytics Findings 20130617 v5.pptx" and "MN UI Fraud Detection - June Meeting with Jim - v7.pptx" and stating that those documents were Deloitte's final deliverables for Wisconsin and Minnesota.
- d. On or about August 19, 2013, while still employed at Deloitte, Sambasivam emailed an internet link and login information to a Sagitec employee for Deloitte's ongoing UI project in Massachusetts.
- e. On or about August 20, 2013, Minkkinen provided a collection of uFACTS

program design documents known as “use cases” from Deloitte’s UI project in Massachusetts to a Sagitec employee to facilitate the development of the Neosurance product.

- f. On or about August 20, 2013, a Sagitec employee sent an email with the subject “uFACTS artifacts” to Minkkinen, Sambasivam, who was still employed at Deloitte, and another Sagitec employee, stating that he “added the captive videos that [they] discussed today morning and uFACTS ERD/DDL’s to the below SharePoint site. Going forward, [he’ll] keep adding additional artifacts to this site[:] <http://sagitecportal/Unemployment%20Insurance/uFACTS/Forms/AllItems.aspx>.” “ERD” means an “Entity Relationship Diagram,” which is a graphical representation of relationships among concepts or events within an information technology (IT) system that assists in defining business processes. “DDL” means “Data Definition Language,” which is used in software to describe data and its relationships in a database.
- g. On or about August 22, 2013, a Sagitec employee sent an email to Sambasivam, while still employed at Deloitte, with the subject line “uFACTS tables needed for development” and an attached spreadsheet. The Sagitec employee wrote, “Attached is the spreadsheet that has all the uFACTS tables that were contained in the DDL’s you sent earlier.”
- h. On or about August 26, 2013, Sambasivam, while still employed at Deloitte, copied the uFACTS Oracle database and later made it available to Sagitec employees to facilitate the development of Neosurance.
- i. On August 29, 2013, a Sagitec employee sent an email with the subject line

“uFACTS code base and all use cases” to two other Sagitec employees and Sambasivam, while still employed with Deloitte. The email stated that “[t]he uFACTS code base from Massachusetts project and all use cases are available at” a specified link located hosted on a Sagitec server in India. Later that day, Sambasivam responded in the email dialogue, stating “[p]lease talk to Deepak before you copy this to other locations.”

- j. On September 2, 2013, a Sagitec employee sent an email to Sambasivam, inquiring about “uFACTS data.” In a response later that day, Sambasivam, while still employed with Deloitte, wrote that “[w]e might have to import the data into a database instance from MN and then [another Sagitec employee] can extract to load into tables with new scheme there.”
- k. On October 15, 2013, Minkkinen emailed Sambasivam a 227-page document prominently labeled “CONFIDENTIAL” on the cover page and “Deloitte Consulting LLP / Confidential – Trade Secret” at the footer on the introductory pages. The document, entitled “uFACTS Solution Framework,” contained a comprehensive explanation of the uFACTS software platform’s functionality. In the email, Minkkinen also wrote “Siva – you could also use this for benefit charges, and other enhancements we need.”
- l. On February 5, 2014, in an email chat dialogue, Minkkinen directed a Sagitec employee to “check how uFACTS coded” a particular software function.
- m. On October 29, 2014, a Sagitec employee sent an email to other Sagitec employees, copying Minkkinen and Sambasivam, with the subject line “Collection use cases from ufacts.” The email stated, “Has all the use cases from



MA and uFACTS, Correspondence specs, reports, etc. that I could find.” Attached to the email was a file named “Collection -use cases.rar,” which contained more than 600 pages of use cases from Deloitte’s project in Massachusetts. Minkkinen responded to the email, asking two Sagitec employees to “analyze this and determine what is feasible for the demonstration.”

- n. On April 13, 2015, Minkkinen sent an email to Sambasivam with the subject “WYCAN pricing,” which attached a spreadsheet entitled “Deloitte Consulting Project Pricing Model” that Deloitte used to determine whether and how to bid on unemployment insurance projects.

### **The Consortium**

16. In 2015, Sagitec won a bid to design, develop, and implement a replacement software system to process UI benefit claims, taxes, and appeals in the states of Maryland and West Virginia. The project was funded by federal grants from the United States Department of Labor (USDOL). The Maryland-West Virginia Consortium (Consortium) contract with Sagitec provided, in pertinent part, that Sagitec “represent[ed], warrant[ed], and covenant[ed]” that its “Work Product, the Software, and the System shall not infringe or otherwise violate any intellectual property or other proprietary rights of a third party.” Minkkinen signed the contract on behalf of Sagitec, and served as the Project Director and primary point of contact for the project. Sambasivam served as the Senior Project Manager. The Consortium contract indicated that Sagitec would be paid between \$49,195,338 and \$70,631,145 for its services. To date, more than \$100 million has been expended on the project.

17. Workforce West Virginia (Workforce WV) is a state government agency funded through the USDOL that oversees the state UI program and a network of workforce development

services. Workforce WV was the state's implementing agency for Sagitec's UI product and thus worked with Sagitec and other subcontractors to develop and install the new UI software platform. Workforce WV employees worked on the UI project in offices in Charleston, Clarksburg, and Morgantown, among other locations in the state, where they often remotely collaborated with Sagitec employees in Maryland and elsewhere.

18. The Maryland Department of Labor, Licensing and Regulation (DLLR) is a state government agency funded through the USDOL that oversees the state UI program throughout Maryland. It was the Maryland DLLR that maintained financial control of the project throughout its duration, and which executed the Consortium contract with Sagitec.

19. In order to facilitate the Consortium project on behalf of Sagitec, Minkkinen, Sambasivam, and ex-Deloitte-current-Sagitec employees/co-conspirators sought, exchanged, and used Deloitte materials in the development of Sagitec's product. Here are a few examples by way of email communications.

- a. In or about October 2015, Minkkinen and Sambasivam are part of an email wherein a Sagitec employee was looking for a specific use case, and states there was not one "from FL or MA in Sharepoint." Minkkinen suggests reaching out to two individuals to obtain the use case, one individual who was still employed at Deloitte.
- b. On or about June 10, 2016, Sambasivam emailed a file entitled "SIDES.zip" to Minkkinen and other Sagitec employees, writing "The attached file has a bunch of documents. Please review them and use them as needed." A review of the SIDES.zip file showed that it exclusively contained documents and files produced for Deloitte's UI projects in Massachusetts and New Mexico.

- c. On or about July 23, 2016, Sambasivam emailed a file entitled “Performance Testing.zip” to a Sagitec employee, writing that “the set of documents I am sending now should give a very good start for finalizing the scenarios for both batch and online with the expected performance numbers.” A review of The Performance Testing.zip showed that it exclusively contained files from Deloitte’s UI project in Massachusetts.

20. After reviewing the evidence and discussing the evidence with CSI Investigator Powers, Affiant is aware of numerous emails in 2015 wherein Minkkinen, Sambasivam, and other ex-Deloitte-current-Sagitec employees/co-conspirators discussed uploading items to, finding items in, and using data from a Sagitec shared site which contained “uFACTS/Forms” in the URL.<sup>4</sup>

#### **BlueJeans by Verizon**

21. As the lead agency with financial control of the Consortium project, the Maryland DLLR also executed contracts with third party subcontractors whose services were necessary to implementation of the project. One of these subcontractors was BlueJeans by Verizon, Verizon Communications. BlueJeans by Verizon (BlueJeans) provided an internet-based communications service which facilitated ongoing meetings and work sessions (virtual meetings) necessary to accomplish various tasks inherent to development of the software and systems which were the ultimate goal of the Consortium project. These virtual meetings frequently included staff from both West Virginia and Maryland, as well as Sagitec employees and subcontractors all on a concurrent basis, and could include thirty or more participants at once, accessing the system from

---

<sup>4</sup> A URL (Uniform Resource Locator) is a compact string of numbers, letters, and symbols that a computer uses to locate a resource on the Internet or on a network.

various states or locations. The virtual meetings allowed all participants to view a common computer screen and to discuss the work at hand on a real time basis.

22. As the lead/contracting agency it was the staff of the Maryland DLLR who typically scheduled BlueJeans virtual meetings, with Maryland DLLR employee Prahalad Patel being the individual who controlled access to the recorded sessions archived by BlueJeans. In an email chain forwarded by Sagitec employee Bernt Peterson to Minkinen on August 10, 2018, Peterson stated, "Pralad manages the bluejeans recordings so he would be the person to contact if you want to review some of them." Sambasivam and others from Sagitec, Workforce WV, and Maryland DLLR were included in the original email chain.

23. On March 18, 2019, CSI Investigator Powers learned from Workforce WV Employee #1 that a BlueJeans virtual meeting had occurred on March 15, 2019, which involved personnel from West Virginia, Maryland, Sagitec, and possibly a subcontractor, CSG. During the meeting there was discussion of a file identified as : I19-UCS-Core-Workflow (2) (1).docx. According to Workforce WV Employee #1, a member of the Maryland DLLR staff participating in the meeting, commented that the metadata for this file identified the originating company as Deloitte, and suggested that Sagitec might want to deal with this. (i.e. That Sagitec should not be in possession of material which originated with its competitor Deloitte.)

24. Workforce WV Employee #1 stated further that a co-worker, Workforce WV Employee #2, was quite upset by this turn of events and drafted an email to a number of individuals within Workforce WV, inclusive of some Workforce management personnel, pointing out what had occurred. Workforce WV Employee #1 subsequently provided CSI Investigator Powers with the March 15, 2019 email generated by Workforce WV Employee #2, with the subject line “Deloitte appears in some of the Use Case documents.” Workforce WV Employee #2 had attached the offending document I19-UCS-Core-Workflow (2) (1).docx to the email, and included the screenshot shown to the right in the body of the email message. Deloitte (highlighted) is listed as the company in the document property information.

Properties	
Size	1.96MB
Pages	64
Words	7912
Total Editing Time	189 Minutes
Title	UCS-I19-Core-Workflow
Tags	Add a tag
Comments	Add comments
Template	Normal.dotm
Status	Add text
Categories	Add a category
Subject	Specify the subject
Hyperlink Base	Add text
Company	Deloitte
Project Phase	Iterative Development
Iteration Activity	Design
Milestone	Milestone 3
Iteration	N/A
Sub-System	MW Consortium
Document ID Value	RYK5VTA2NDS4-11828013...
Description	Add text
Related Dates	
Last Modified	Yesterday, 11:11 AM
Created	1/30/2019 10:19 PM
Last Printed	11/12/2017 3:49 PM
Related People	
Manager	Specify the manager
Author	PB Peterson, Bernt
	Add an author
Last Modified By	PJ Parsons, Jeremy R

25. In the email, Workforce WV Employee #2 stated, “Also, this is not the only document to have Deloitte as the Company. I found Deloitte in some other documents that I had previously downloaded to my PC.”

26. Affiant has reviewed the metadata for I19-UCS-Core-Workflow (2) (1).docx, and confirmed that, as in the screenshot, the properties tab identified the company as Deloitte.

27. CSI Investigator Powers advised Affiant that during a witness preparation session conducted at the U.S. Attorney’s offices in Charleston, West Virginia on August 10, 2023, with

Workforce WV employee Jonathan Link, Mr. Link recounted statements made during a BlueJeans virtual meeting which to the best of his recollection occurred circa September or October of 2018. Mr. Link recounted that one of the participants in this BlueJeans virtual meeting was Sagitec employee Marcel Mascarenhas. Mr. Link recalled that he asked Mascarenhas “does Sagitec own the software,” to which Mr. Mascarenhas responded, “there was an agreement between David Minkkinen and Deloitte to take the code and personnel with him.” (i.e. when Minkkinen left Deloitte in 2013.)

#### **Existence of BlueJeans by Verizon Recordings**

28. After the August 2023 preparation session, the government attempted to determine whether the recordings of the above referenced virtual meetings existed. Representatives of Workforce WV indicated that they did not maintain or currently have access to the recordings. The government was unable to determine whether the Maryland DDLR had copies of or access to the recordings, so it reached out to BlueJeans by Verizon. Representatives of Verizon Communications have acknowledged that virtual meetings associated with the Target Accounts, including the identities of those participating, were electronically recorded and maintained by BlueJeans by Verizon. Representatives of Verizon Communications also reported they are in possession of 7,000 recordings covering a period from 2016 to 2020, related to the Consortium project. On September 27, 2022, the government served Verizon with a request under 18 U.S.C. § 2703(f) to preserve the **Target Recordings**. Pertinent to this affidavit for a search warrant, BlueJeans by Verizon acknowledged that it does have in its possession: a) the recording of a BlueJeans virtual meeting from March 15, 2019; and b) ten recordings of BlueJeans virtual meetings conducted between August 2018 and November 2018 in which Workforce WV employee Jonathan Link and Sagitec employee Marcel Mascarenhas were

among the participants. Thus, the government is seeking to seize and search only eleven recordings.

29. Notably, per an August 16, 2023, blog<sup>5</sup> posted on the bluejeans.com website, Bluejeans by Verizon announced that its “products and services will be retired in the first half of 2024. Timelines for service availability will vary.” The site also represented that existing customers could continue to use their “BlueJeans services as usual for now.” Thus the government seeks to seize and search as soon as possible any BlueJeans by Verizon recordings over which it has probable cause, i.e. the **Target Recordings**.

### **The Federal Investigation**

30. Shortly after the CSI received information in 2016 from a Workforce WV employee raising questions about the Consortium project and more specifically whether Sagitec might have stolen and used trade secret material from Deloitte, the DOL-OIG joined the investigation in 2017. This joint investigation continues to the present date and has involved extensive interviews with, among other individuals: current and former staff of Workforce WV, the Maryland DLLR, Sagitec, and Deloitte. Affiant has reviewed the evidence and reports of interviews of various WorkForce WV employees, revealing that the WorkForce WV employees working on the Consortium project often identified references to Deloitte or Deloitte’s clients such as Massachusetts or New Mexico (zip codes, phone numbers, cities or counties) embedded within Sagitec’s Neosurance product.

31. The investigation also has involved the gathering and analysis of massive amounts of electronic mail and associated attachments, along with other documentation associated with the Consortium project, some of which was gathered by employees of Workforce

---

<sup>5</sup> <https://www.bluejeans.com/blog/bluejeans-being-sunset>.



WV. In addition to the government's investigation, Sagitec initiated its own internal investigation of the matter, conducting internal interviews and gathering documentation and electronic mail as well. The results of Sagitec's efforts have been provided to the Government and are part of the Government's evidence gathered in this matter.

32. CSI Investigator Powers and Affiant have reviewed the various statements made by Minkkinen and Sambasivam (in letters, emails, and through interviews and summaries of interviews) when confronted with allegations regarding the theft of Deloitte intellectual property. Over the course of the investigation, Minkkinen explicitly and repeatedly denied that he or Sagitec even possessed any Deloitte data. As a few examples, Minkkinen stated:

- a. that neither he nor any former Deloitte-employee-now-employed-by-Sagitec had “retained any software, source code, or any other tangible artifacts authored by Deloitte, a Deloitte subcontractor or consultant, or a Deloitte client after leaving Deloitte's employment;”
- b. “the allegation that Sagitec has in any way misappropriated another party's property is defamatory;”
- c. that Sagitec had not “obtained copies of any software, source code, or any other tangible software artifacts authored by Deloitte, a Deloitte subcontractor or consultant, or a Deloitte client after leaving Deloitte's employment;”
- d. any accusation that he took any Deloitte materials and brought them to Sagitec was “entirely false;”
- e. that he assured the CSI Investigator and a USDOL Special Agent that “nothing of Deloitte technology was used in [Sagitec's] solution, period;” and



- f. “if somebody was using the [Deloitte] use case from another state I’m not aware of it.”

Over the course of the investigation, Sambasivam admitted to CSI Investigator Powers and a USDOL Special Agent, that he observed Minkkinen in possession of some Deloitte material, but denied that he (Sambasivam) personally took any Deloitte materials from Deloitte.

33. Post indictment, the defense has raised additional contradictory defenses, to include that others may be responsible for obtaining the Deloitte materials, that Minkkinen had permission from Deloitte to take the materials, that the materials were not used by Sagitec in developing Sagitec’s product, that the materials were not proprietary, etc. Based upon the facts presented herein, it is Affiant’s belief a search of records in the possession BlueJeans by Verizon, Verizon Communications will produce evidence confirming Minkkinen’s and Sambasivam’s knowledge of their possession and use (and thus Sagitec’s possession and use) of proprietary materials belonging to Deloitte.

#### **BLUEJEANS BY VERIZON**


34. BlueJeans was a software company founded in 2009, that provided interoperable cloud-based video conferencing services for a fee to individuals and small to medium sized businesses. In April 2020, Verizon Communications (Verizon) partnered with BlueJeans to assist BlueJeans expand its market reach and improve its services. Although BlueJeans is headquartered in San Jose, California, Verizon maintains access to the recordings from, and can be served at 180 Washington Valley Road, Bedminster, NJ 07921.

#### **CONCLUSION**

35. Based on the forgoing, I request that the Court issue the proposed search warrant.

36. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Verizon. Because the warrant will be served on Verizon, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

  
\_\_\_\_\_  
JEFFREY CARTER  
Special Agent  
United States Department of Labor  
Office of Inspector General

Subscribed and sworn to before me on October 20, 2023.

  
\_\_\_\_\_  
Honorable Omar J. Aboulhosn  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with the BlueJeans by Verizon accounts bearing BlueJeans IDs 169152207, 2336004334, 2483755327, and 9164987431, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on September 27, 2023, stored at premises owned, maintained, controlled, or operated by Verizon Communications (Verizon), an electronic communications service and/or remote computing service provider headquartered at 180 Washington Valley Road, Bedminster, NJ 07921.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by BlueJeans by Verizon / Verizon Communications**

To the extent that the BlueJeans by Verizon accounts (Target Accounts) described in Attachment A are within the possession, custody, or control of Verizon Communications (Verizon), regardless of whether such information is located within or outside of the United States, and including any records, files, logs, or information that has been deleted but is still available to Verizon, Verizon is required to disclose to the government the following:

- a. The recordings of the virtual meetings from the Target Accounts which occurred between August 1, 2018, and November 30, 2018, *and* which included both Jonathan Link and Marcel Mascarenhas as participants;
- b. The recording(s) of the virtual meeting(s) associated with the BlueJeans ID 2483755327, which occurred on March 15, 2019, at or around 4:05 pm Eastern Daylight Time; and
- c. any subscriber information associated with the Target Accounts as related to the **Target Recordings** referenced in paragraphs (a) and (b) above.

**II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 1832(a)(5) (conspiracy to commit trade secret theft); 18 U.S.C. § 1349 (18 conspiracy to commit wire fraud in violation of 18 U.S.C. § 1343); and 18 U.S.C. § 1001(a)(2) (making a false statement to a federal agent) by David Minkinen and Sivaraman Sambasivam, pertaining to the following matters:

- a. discussions regarding any possession by Sagitec of Deloitte data;

- b. discussions regarding or references to the existence of metadata identifying:
  - 1. Deloitte as the company;
  - 2. a Deloitte employee as the author; or
  - 3. a date of creation or printing prior to 2013/
- c. discussions regarding or references to Deloitte, uFACTS, or Deloitte clients: such as Massachusetts, New Mexico, and Florida.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC  
RECORDS PURSUANT TO FEDERAL RULES OF  
EVIDENCE 902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Verizon Communications (Verizon), and my title is \_\_\_\_\_. I am qualified to authenticate the records from BlueJeans by Verizon because I am familiar with how the records were created, managed, stored, and retrieved. I state that the BlueJeans by Verizon records [**contained on the USB device marked (describe) \_\_\_\_\_**] hereto are true duplicates of the original records in the custody of BlueJeans by Verizon. The produced records consist of subscriber information and recordings of virtual meetings. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of BlueJeans by Verizon (BlueJeans) or Verizon, and they were made by BlueJeans or Verizon as a regular practice; and

b. such records were generated by BlueJeans' or Verizon's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of BlueJeans or Verizon in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by BlueJeans or Verizon, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date: \_\_\_\_\_ Signature: \_\_\_\_\_

Name Printed: \_\_\_\_\_